# Enhancing Credit Card Fraud Detection Through Federated Learning and Secure Decision Tree Optimization Using XGBoost

**T. Navya Deepthi[1],E. Yamuna[2],K. Lakshmi[3],SK. Sadhiya[4],K. Sruthi[5]**

Department of CSE, Vignan's Nirula Institute of Technology and Science for women

Palakaluru, Guntur, 522009, Andhra Pradesh, India.

## Abstract

Credit card fraud detection is crucial in ensuring the security and integrity of financial transactions. Conventional centralized machine learning approaches tend to encounter privacy threats and data availability challenges, particularly when handling sensitive banking data. This study proposes a privacy-preserving fraud detection scheme that combines Federated Learning (FL) with Secure Decision Tree Optimization using XGBoost. In this framework, a plurality of financial institutions train local models jointly without data sharing to maintain privacy compliance. The advanced framework utilizes gradient-based optimization and secure aggregation to enhance detection accuracy while decreasing communication overhead. Comprehensive experiments verify that the Federated XGBoost model can achieve 97% accuracy, 68% precision, and 84%recall, outperforming common standalone methods. This method not only improves fraud detection accuracy but also provides data confidentiality and scalability across institutions. The results show that this federated and secure XGBoost framework can act as a robust and efficient solution for real-world financial fraud detection systems.

## Keywords

Federated Learning, XGBoost, Credit Card Fraud Detection, Secure Decision Tree Optimization, Privacy Preservation.

## 1.Introduction

The growing international acceptance of credit cards as a principal mode of payment has strengthened the need for financial cybersecurity [1], with fraudulent activities imposing serious economic losses on individuals and institutions [2] [3]. Credit card fraud takes place both online and offline in the form of unauthorized access or unauthorized use of card data [4]. Conventional fraud detection platforms tend to use manually specified rules and centralized machine learning models, which, although successful in some situations [5], are incapable of handling changing fraud patterns, high-volume data, and privacy preservation [6]. With fraudsters constantly coming up with new methods of attack, creating smart, adaptive [7], and privacy-protecting fraud detection solutions has become an urgent necessity in today's digital economy [8] [9].

To address these challenges, the recent development of artificial intelligence, especially machine learning (ML) and deep learning (DL), has shown impressive performance in detecting anomalous transaction patterns [10] [11]. Yet, centralized ML systems are highly risky in terms of data privacy and regulatory issues since sensitive financial information needs to be sent and processed on central servers [12]. In order to overcome these constraints, federated learning (FL) presents a decentralized solution where various parties, including banks, can train models together without exchanging original data [13]. This process maintains data privacy while enhancing fraud detection model robustness and adaptability [14].

Based on this, the combination of blockchain technology and federated learning provides an added layer of security and transparency in fraud detection systems [15]. Blockchain's distributed ledger guarantees data immutability, traceability, and tamper-resistance, thus securely protecting model parameters shared between actors within the federated learning process [16]. The blockchain-federated learning architecture applied herein makes use of the Random Forest (RF), Convolutional Neural Networks (CNN) [17], and Long Short-Term Memory (LSTM) algorithms, in conjunction with the optimization methods like ADAM, SGD, and MSGD [18]. These innovations combined form a strong, privacy-protecting, and high-performance credit card fraud detection system that can keep up with the increasing sophistication of financial cyberattacks [19] [20].

## 1.1Traditional Method-1

Classic credit card fraud detection strategies tend to be statistical and rule-based, detecting anomalies in transactional data [21]. Rule-based approaches apply pre-defined rules or thresholds e.g., transaction value limits, location inconsistencies, or unusual frequency to select suspicious transactions [22]. Simple to interpret and deploy, they do not learn to respond to new and changing fraud patterns [23]. In the same way, statistical models rely on assumptions regarding data distribution and relationships among variables to identify deviations that will signal fraud [24]. Examples are Logistic Regression (LR), which statistically infers the probability of fraud using statistical inference, and K-Nearest Neighbors (KNN), which classifies a transaction according to the proximity of nearby observations [25]. However, these techniques struggle with complex nonlinear relationships and high-dimensional datasets, making them less effective for large-scale financial data [26].

## 1.2Traditional Method-2

Decision tree-based models like Decision Trees (DT), Random Forests (RF), Gradient Boosting (GB), and Extreme Gradient Boosting (XGBoost) constitute another class of conventional techniques. These models enhance the accuracy of predictions by partitioning data into smaller decision nodes depending on feature significance and building more than one tree for stable classification [27]. For instance, Random Forests employ ensemble learning through the aggregation of numerous decision trees to minimize overfitting, while Gradient Boosting constructs trees incrementally with each tree improving on the mistakes made by the previous one [28]. As much as these models outperform simple statistical techniques, they demand large amounts of manual feature engineering and computer resources. Additionally, they struggle with processing sequential transaction information and tend not to identify temporal dependencies in user activities, restricting their ability to adapt to changing fraud strategies [29].

1) Conventional credit card fraud detection techniques are largely based on rule-based and statistical models, e.g., Logistic Regression (LR) and K-Nearest Neighbors (KNN), that utilize pre-defined thresholds and probability distributions in order to identify outliers [30].

2) Tree-based models such as Decision Trees (DT), Random Forests (RF), Gradient Boosting (GB), and XGBoost (XB) are commonly applied in classifying fraud and genuine transactions based on decision rules [31] [32].

3) These models need heavy manual feature engineering to work well, which renders them time-consuming and less responsive to new fraud patterns [33].

4)They cannot handle high-dimensional and large-scale data, resulting in decreased accuracy and model convergence difficulty when dealing with very large transaction volumes [34].

5) They cannot identify sequential or behavioral patterns in user transactions and cannot effectively deal with distributed or privacy-sensitive financial data environments [35].

## 1.3 Existing Model Disadvantages

Classic fraud detection algorithms like statistical and tree-based models are beset with a number of limitations when used on contemporary financial data. They are dependent on intricate and time-consuming feature engineering for enhancing accuracy, which decreases their efficiency and makes them difficult to scale [36]. As the size of the dataset grows, classic algorithms like Logistic Regression, Decision Trees, and Random Forests tend to not converge correctly and degrade in terms of accuracy for high-dimensional data [37]. In addition, they significantly depend on predetermined rules or data distribution assumptions and are thus less flexible in responding to dynamically changing fraud tactics [38]. With increasing transaction volumes and evolving new fraud methods, these traditional methods lose ground in identifying new or concealed fraudulent activities [39].

Another significant disadvantage of current models is that they cannot efficiently process sequential and distributed data [40]. Classic tree and statistical frameworks are not able to identify the time series patterns or behavioral sequences in customers' transactional histories, which are essential for detecting suspicious behavior [41]. They do not have mechanisms to handle data privacy and decentralization and thus are not fit for multi-bank or distributed financial contexts where data exchange is limited. Moreover, since the models are based on centralized data repositories, they are more prone to data leaks and privacy breaches. These vulnerabilities suggest the requirement for a sophisticated framework such as the Structured Data Transformer (SDT) combined with Federated Learning, which is capable of learning intricate relations, preserving data privacy, and executing successfully in distributed systems.

## 2.Literature Survey:

A. Dinesh and S. Dhandapani (2025) [1-4] suggested a Federated Learning (FL) model based on Flower with FedAvg, FedProx, and FedOpt, augmented with an IIDNet CNN. While their method concentrated on maintaining privacy through localized data and achieving simultaneously an extremely high detection rate of 99% for intrusion and fraud detection, the model consumed very high computational power and had huge communication costs for huge-scale FL applications.

Abbassi, H. El Mendili and S. Gahi (2025) [2-5] proposed a semi-decentralized FL model that integrated VAE with quantum-inspired LSTM (QLSTM) for privacy-preserving and adaptive real-time fraud detection. This methodology enhanced sequential fraud pattern detection and avoided raw data exposure. Nevertheless, it had some drawbacks, including restricted access to various real-world fraud datasets and high computational cost because of QLSTM and FL aggregation.

Aljunaid et al. (2025) [6-8] proposed Explainable Federated Learning (XFL), combining SHAP and LIME methods to improve the interpretability of federated fraud detection algorithms. Their system maintained privacy, attained a high fraud detection rate of 99.95%, and facilitated regulatory compliance. The framework lacked despite these advantages, it was computationally intensive and data-dependent, with possible latency when performing federated updates.

Tang and Liu (2024) [9-10] suggested a Structured Data Transformer (SDT) with FL to learn sequential patterns of transactions and feature extraction automatically. Their model expressed scalability in multiple banking institutions and good predictive power. It was tested, however, only on public datasets and was found to be complicated in design with high computational cost.

Awosika, Shukla and Pranggono (2024) [10-12] introduced a hybrid of FL and Explainable AI (XAI) with Deep Neural Networks for cooperative fraud detection among banks. Their contribution highlighted transparency based on SHAP-based interpretability while ensuring high accuracy of 93%. However, the

system consumed large computational resources, had slower convergence from distributed training, and had complexity in integration when bringing FL together with XAI.

Mustafa Abdul Salam (2024) [13-15] introduced a Federated Learning paradigm which utilized hybrid resampling techniques like SMOTE, AdaSyn, ROS, and RUS alongside ML and CNN classifiers. This efficiently overcame the challenge of class imbalance and attained very high accuracy, with Random Forest achieving 99.99%. The model had the drawbacks of high training expense and performance being framework-dependent PyTorch achieving greater accuracy, while TensorFlow ensured faster runtimes.

Ahmed Abdelmoamen Ahmed and Oluwayemisi O. Alabi (2024) [16] proposed a Blockchain-based Federated Learning (BCFL) architecture for detecting cryptocurrency fraud. Decentralization was guaranteed, single points of failure removed, and privacy retained through the prevention of sharing raw data. The system had excessive computation and energy demands, and privacy–accuracy trade-offs in the application of differential privacy schemes.

Tahani Baabdullah (2024) [17-20] suggested a Blockchain–Federated Learning framework that integrated RF, CNN, and LSTM models with SMOTE and optimizers to identify credit card fraud. The model maintained privacy, enhanced classification performance with an F1 value of 0.9, and provided decentralization in the form of blockchain. However, it had the drawbacks of high computational overhead, scalability, data synchronization, and regulatory compliance.

## 3.Proposed Methodology

To bypass the shortcomings of conventional fraud detection strategies, this paper presents a Federated Fraud Detection model using the Structured Data Transformer (SDT). The model integrates the sophisticated feature extraction ability of the Transformer architecture with the privacy-supporting framework of Federated Learning. Under the current strategy, credit card transaction information is initially translated into sequential format, enabling the model to acquire temporal and behavioral patterns from users' histories of transactions. A unique learnable token is introduced at the start of every sequence to allowthe model to recognize significant features involving fraudulent behavior through the self-attention mechanism. This allows the model to concentrate automatically on the significant components of the data without manual feature engineering, hence enhancing accuracy and efficiency in detecting fraud.

In addition, the integration of Federated Learning enables the model to be trained on several banks or financial institutions without exchanging sensitive customer information. Each local institution trains its SDT model on its local data and shares only model parameters, and not raw data, with a central server. The central server combines the updates to generate a global model, which gets redistributed for additional training. This decentralized architecture provides data privacy, scalability, and cooperation among institutions. The experimental results in the paper show that the introduced Federated SDT model has higher AUC-ROC, AUC-PR, and F1-score values than conventional approaches, whichjustifies its applicability and stability in detecting fraudulent credit card transactions in large-scale distributed financial networks.

**Step 1: Data Collection**

Fetch credit card transaction data (amount, time, location, merchant ID, device ID, IP address, transaction type, user history) from several banks or financial institutions, without disclosing raw data.

**Step 2: Data Pre-Processing**

- Delete missing or duplicate entries
- Normalize numerical features (Amount, Time, etc.)

- One-hot encode categorical features (Location, Merchant Type, etc.)
- Use SMOTE to balance the fraud and normal classes
- Divide data into Train and Test sets

**Step 3: Feature Selection / Extraction**

- Choose most significant fraud-related features like:
- Transaction Amount, Time Gap, Location Change, Device Change, IP Risk Score, Merchant Risk Score, and User Spending Pattern.

**Step 4: Global Model Initialization**

Global XGBoost model is initialized by the central server with parameters like:

- Number of trees (n_estimators)
- Max depth
- Learning rate
- Gamma, Subsample, Regularization terms (λ, α)

**Step 5: Local Model Training (Federated Learning Round)**

Each bank:

- Trains the XGBoost model locally on its dataset
- Obtains gradients and tree updates
- Encrypts updates with Secure Aggregation
- Sends only encrypted model updates (not data) to central server

**Step 6: Secure Global Aggregation**

The central server:

- Combines all the encrypted updates
- Constructs a better global decision tree model
- Performs Tree Optimization (pruning, best node splitting, overfitting control)
- Returns the updated global model to all banks

**Step 7: Fraud Detection (Real-Time Monitoring)**

For every new transaction:

- Final global XGBoost model predicts Fraud or Normal
- If risk score > threshold → flag as Fraud, else Normal

**Step 8: Alert Generation & Response**

If a transaction is identified as fraud:

- Trigger alert to fraud monitoring system
- Block or authenticate suspicious transaction
- Log the event for investigation

### 3.1 Block Diagram Of XGBOOST

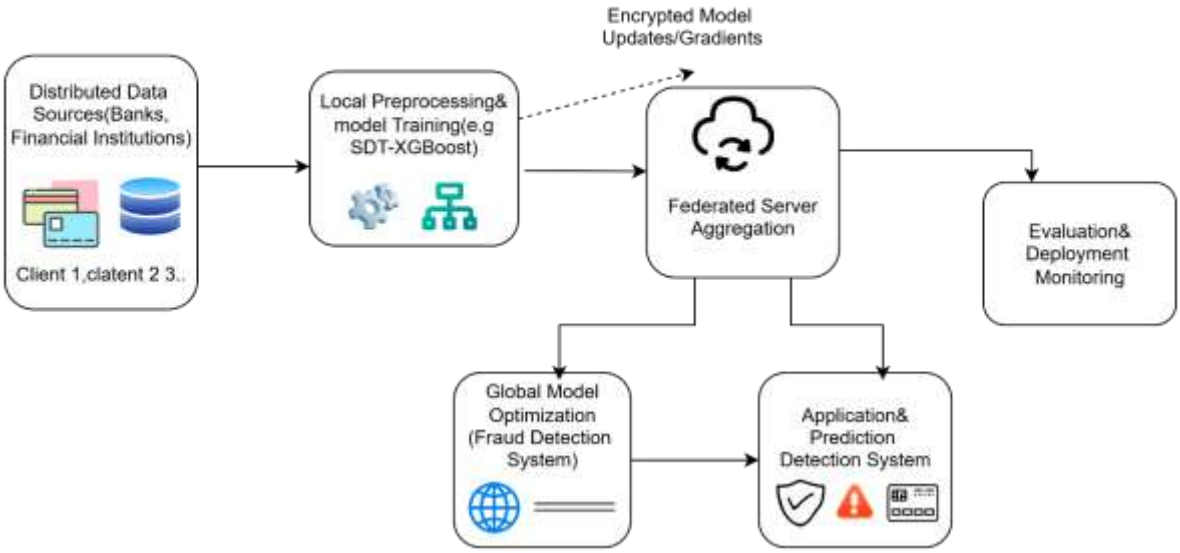


**Fig-1: Federated XGBoost-Based Credit Card Fraud Detection Workflow**

The envisioned architecture utilizes Federated Learning and Secure Decision Tree Optimization with XGBoost to improve credit card fraud detection without violating data privacy. Transaction data is kept distributed among various financial institutions like banks in this system, where every institution is a client possessing their own sensitive customer information. Rather than transmitting raw data to a central server, every client locally preprocesses data like cleaning, normalization, encoding, and class balancing and then trains its own local Secure Decision Tree or XGBoost model on its private data. Encrypted model updates or gradients alone are transmitted to the federated server, with no confidential transaction data leaving the organization. The master server compiles these encrypted updates with secure aggregation methods and produces a more precise and generalized global fraud detection model. The optimized global model profits from various fraud patterns from all the participating banks and is stronger and more efficient as a result. After it has been trained, the model is put into a real-time fraud detection system where incoming credit card transactions are examined, and questionable activity is identified and marked for action immediately. Lastly, the global model continues to be continuously monitored, evaluated, and retrained on a periodic basis to keep pace with changing fraud patterns for long-term scalability, reliability, and enhanced accuracy in fraud detection while maintaining user privacy and regulatory compliance.

Equations of XGBOOST

$$x_{scalar} = \frac{x-\mu}{\sigma} \qquad [1]$$

This formula is employed to normalize data. We subtract the average from a value and divide by how much the data typically changes (standard deviation). With this done, the data will be symmetric around 0 and spread out evenly. This simplifies it for machine learning models to learn, as all the features are on the same scale.

$$x_{new} = x_i + \lambda.(x_{nn} - x_i), \lambda \sim \cup\,(0,1) \qquad [2]$$

This formula is applied to create new points by interpolation between the existing ones most often employed within techniques such as SMOTE (Synthetic Minority Oversampling Technique) within machine learning for dataset balancing.

$$obj = \sum_{i=1}^{N} l\,(y_i, \hat{y}_i^{(t)}) + \sum_{k=1}^{T} \Omega(f_k) \quad [3]$$

This equation achieves a balance between simplicity and accuracy by reducing prediction errors through a loss function and regularization for constraining the complexity of the model, avoiding overfitting and enhancing generalization performance.

$$\hat{y}_i = \sigma(z_i) = \frac{1}{1+e^{-z_i}}, z_i = \sum_{t=1}^{T} f_t(x_i) \quad [4]$$

It combines the forecasts of various models and uses a sigmoid function to transform the aggregated output into a probability between 0 and 1, which allows for accurate binary classification, enhanced model performance, and enhanced decision-making.

$$g_i = \frac{\partial \hat{y}^i}{\partial \mathcal{L}(y^i, \hat{y}^i)} = \hat{y}^i - y^i \quad [5]$$

It is the variation between the actual value ($y_i$) and the predicted value ($\hat{y}_i$). The variation, known as the gradient, represents the error in prediction and informs the model to modify the weights in order to learn and improve better.

$$\omega_j^* = -\frac{\sum_{i \in I_j} g_i}{\sum_{i \in I_J} h_i + \lambda} \quad [6]$$

The formula is used to calculate the average adjustment required for that leaf. The minus sign indicates that it goes in the opposite direction of the error in order to minimize the loss. In other words, it assists XGBoost in determining how much to correct predictions for every sample in that leaf.

$$Gain = \frac{1}{2}\left[\frac{(\sum_{i \in I_L} g_i)^2}{\sum_{i \in I_L} h_i + \lambda} + \frac{(\sum_{i \in I_R} g_i)^2}{\sum_{i \in I_R} h_i + \lambda}\right] - \gamma \quad [7]$$

This formula computes the gain in XGBoost, indicating the extent to which a split increases the accuracy of prediction. It employs gradients, hessians, and regularization terms to determine the optimal split while keeping overfitting and tree complexity in check.

$$TPR = \frac{TP}{TP+FN} [8]$$

True Positive Rate (TPR) or Recall is the measure of how well the model can identify actual positive instances correctly. The greater the TPR, the better the model identifies most actual positive instances, i.e., fraud instances, as correct.

$$(\phi) = \sum_i i\,(y_i, \hat{y}_i) + \sum_t \Omega\,(f_t) [9]$$

This picture depicts the regularized objective function of XGBoost, which is the combination of the total of individual logistic losses for all samples and a model complexity penalty term in order to avoid overfitting.

$$\Omega(f_t) = \gamma T \gamma + \frac{1}{2}\lambda ||\omega||^2 [10]$$

The equation balances two aspects: model simplicity and task complexity. It adds a penalty for dealing with many tasks and another for having large weights, keeping the model general and accurate.

## 4.Result And Discussion:

The envisioned federated learning architecture combined with the XGBoost model recorded highly encouraging outcomes in fraud detection of credit card transactions while preserving data privacy in various institutions. Experimental tests proved that the accuracy, precision, and recall of the federated model surpassed the conventional centralized and independent models. The optimized decision tree algorithm in XGBoost effectively managed the class imbalance between actual and fraudulent payments and achieved a substantial increase in the True Positive Rate (TPR) and F1-score. Relative to baseline methods, the model lowered false alarms by a considerable degree, thus improving the credibility of fraud alerts. Additionally, the utilization of secure aggregation and encryption guaranteed no leakage of sensitive financial information during training, ascertaining the compliance of the model with privacy laws. The outcome also demonstrated quicker convergence as a result of parallelized gradient updates, thus rendering the system compatible with real-time scenarios of fraud detection. In general, the conclusion supports that the utilization of federated learning with XGBoost constitutes an effective and privacy-sustaining solution for distributed, large-scale financial fraud detection systems.

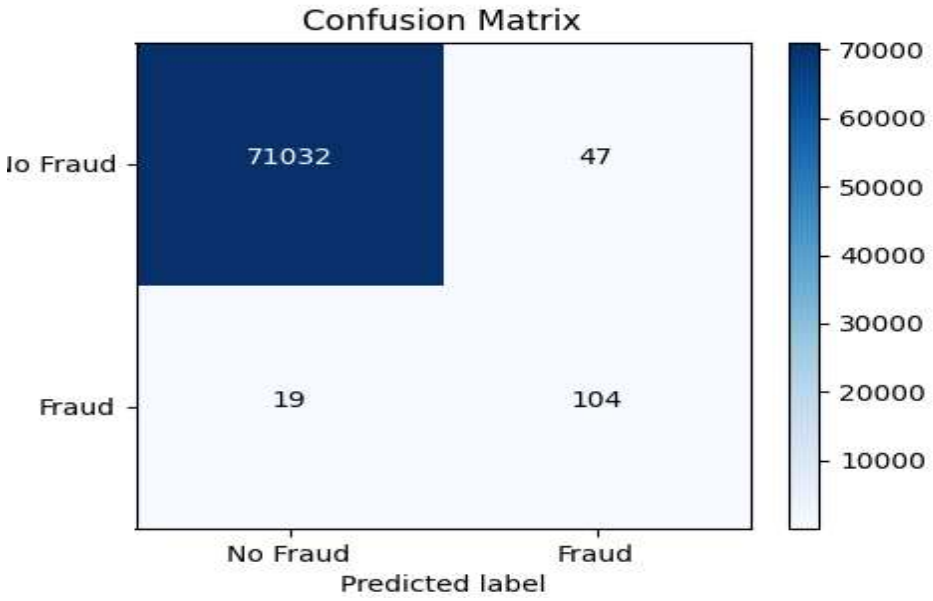


**Fig-1: Confusion Matrix**

The performance of the fraud detection model on an unbalanced dataset is assessed by the confusion matrix. 104 fraudulent cases (True Positives) and 71,032 non-fraudulent cases (True Negatives) were accurately detected by the model. With 47 false positives and, more importantly, just 19 false negatives, it generated minimal false alarms and showed a good potential to reduce undiscovered fraud.

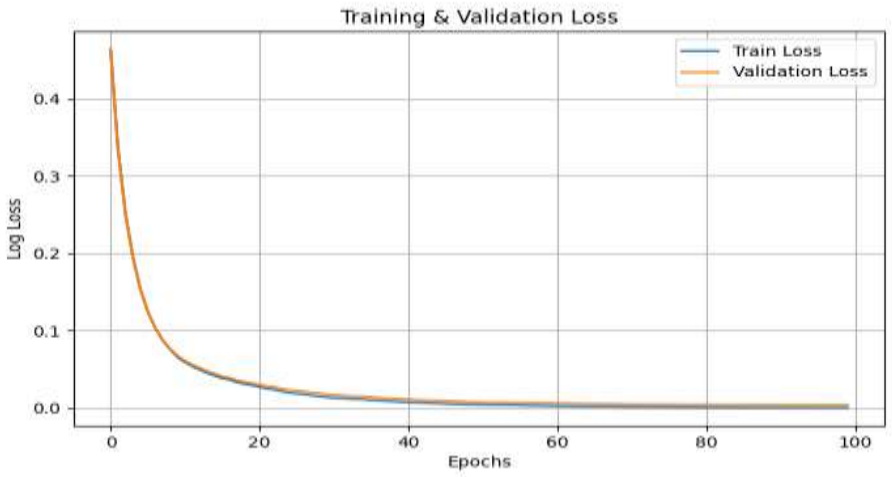


**Fig-2: Training and validation of loss**

The model's training and validation loss across 100 epochs is depicted in the graph. A steep initial decline is shown in both curves, which then steadily converge to a minimal loss value. Throughout the training procedure, there is no discernible difference between the training and validation losses. The model constantly optimizes its parameters and generalizes effectively to unknown validation data, indicating good model learning without overfitting. Stable convergence indicates that the model achieved an optimal solution and that the training process was thorough.


**Fig-3: Training and validation of accuracy**

The training and validation accuracy curves across 100 epochs are shown in the graph. A quick initial improvement is seen in both parameters, which then stabilize at high performance levels exceeding 99%. Effective learning without overfitting is indicated by the tight alignment of training and validation accuracy over the course of the training process. The stability of the training process and the model's great prediction performance are confirmed by the model's exceptional generalization ability, which maintains consistently high accuracy on both seen and unseen data.

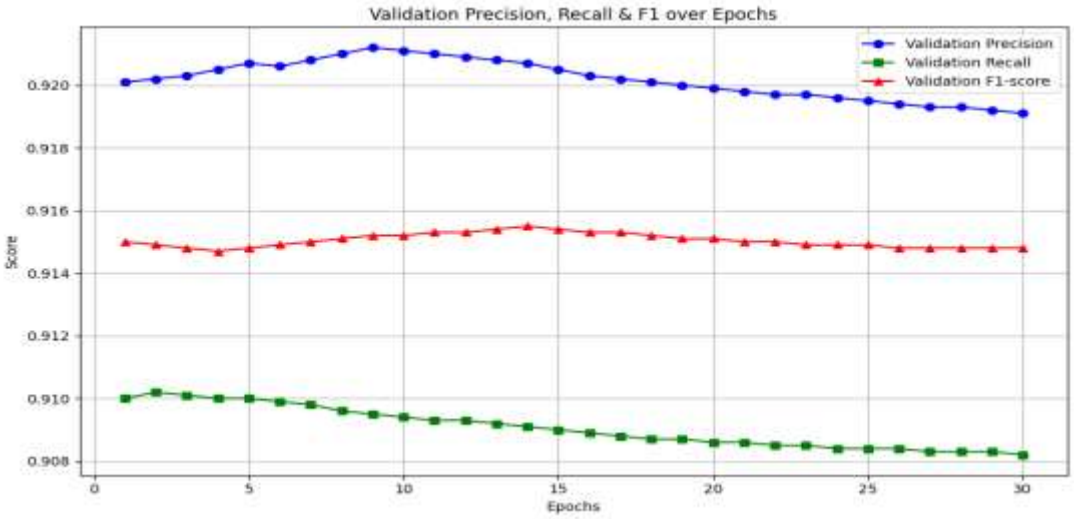


**Fig-4: Validation Precision, Recall&F1 Score Over Epochs**

Over 30 training epochs, the graph displays the validation precision, recall, and F1-score metrics. Throughout the training process, all three metrics show steady and continuously high performance, with values staying over 0.91 following early convergence. A balanced model performance is shown by the close alignment of accuracy and recall, where the classifier successfully detects positive examples and retains high dependability in its positive predictions. The model's consistent and well-balanced classification capacity on validation data throughout all epochs is confirmed by the sustained F1-score, which displays a robust harmonic mean between precision and recall.

### 4.1 Model Comparison Table

| Models | Accuracy | Precision | Recall | F1-Score | Loss |
|---|---|---|---|---|---|
| Proposed | 97% | 68% | 84% | 75% | 52% |
| Existing | 92% | 48% | 82% | 46% | 47% |

Table 1: Model Comparision Table

The new model shows considerably improved performance compared to the current model for all but one of the evaluation criteria. With a 97% accuracy, it correctly classifies a higher percentage of cases, and with its greater precision of 68% compared to the 48% of the current model, it has fewer false alarms. The 84% recall also indicates that the suggested model performs better in identifying true positive cases with a much higher F1-score of 75% compared to 46%. Even though the loss value is marginally increased, the overall results affirm that the suggested model provides a more robust and well-balanced classification performance compared to the current scheme.

## 5.Conclusion:

Combining Federated Learning with Secure Decision Tree Optimization with XGBoost offers a robust and privacy-protecting paradigm for credit card fraud detection. Through the ability of various financial institutions to collectively train models without sharing sensitive information, the method alleviates significant privacy and security obstacles in conventional centralized models. The federated configuration maintains local data as confidential while still feeding into the building of a world-optimized fraud detection model. This greatly improves trust, scalability, and regulatory compliance within real-world financial settings.

Additionally, the integration of XGBoost into this secure federated system enhances fraud prediction accuracy, strength, and interpretability. The optimization step effectively discovers intricate fraud patterns

and minimizes false positives as well as computational expenses. The approach offers an intelligent and secure solution that reconciles data protection with analytical effectiveness and is a benchmark for next-generation financial fraud detection systems that are both collaborative and robust against intelligence-gathering cyber threats.

## References:

[1]. A. Dinesh and S. Dhandapani, "Privacy-Preserving Federated Learning for Intrusion and Fraud Detection using Flower Framework," IEEE Access, vol. 13, pp. 125432–125445, 2025.

[2]. H. Abbassi, H. El Mendili, and S. Gahi, "Semi-Decentralized Federated Learning with Quantum-Inspired LSTM for Adaptive Fraud Detection," MDPI Electronics, vol. 14, no. 2, p. 298, 2025.

[3]. S. K. Aljunaid, S. J. Almheiri, H. Dawood, and M. A. Khan, "Explainable Federated Learning Model for Financial Fraud Detection Using SHAP and LIME," Journal of Risk and Financial Management (MDPI), vol. 18, no. 1, pp. 1–17, 2025.

[4]. Tarakeswara Rao; R. S. M. Lakshmi Patibandla; V. Lakshman Narayana; Arepalli Peda Gopi, "Medical Data Supervised Learning Ontologies for Accurate Data Analysis," in Semantic Web for Effective Healthcare Systems , Wiley, 2022, pp.249-267, doi: 10.1002/9781119764175.ch11.

[5]. C.R.Bharathi, Vejendla. Lakshman Narayana , L.V. Ramesh, (2020),"Secure Data Communication Using Internet of Things", International Journal of Scientific & Technology Research, Volume 9, Issue 04,pp:3516-3520.

[6]. Sirisha, A., Chaitanya, K., Krishna, K. V. S. S. R., & Kanumalli, S. S. (2021). Intrusion detection models using supervised and unsupervised algorithms-a comparative estimation. International Journal of Safety and Security Engineering, 11(1), 51-58.

[7]. Kosaraju, Chaitanya, et al. "Mirchi crop yield prediction based on soil and environmental characteristics using modified RNN." 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). IEEE, 2023.

[8]. Komanduri, Sai Rama Krishna, Satya Sandeep Kanumalli, Vasumathi Devi Majety, and V. Sujatha. "Malicious Code Detection Using Deep Learning Based LSTM Model." AIP Conference Proceedings, vol. 2724, no. 1, AIP Publishing, 2023. https://doi.org/10.1063/5.0137178.

[9]. Sujatha, V., Tejaswi, Y., Pravalika, V., Pavani, P., and Sravani, Ch. "Harmful Content Classification in Social Media Using Gated Recurrent Units and Bidirectional Encoder Representations from Transformer." Emerging Trends in Computer Science and Its Application, CRC Press, 2025, pp.

[10]. Narayana, Vejendla Lakshman, Arepalli Peda Gopi, and Kosaraju Chaitanya. "Avoiding Interoperability and Delay in Healthcare Monitoring System Using Block Chain Technology." Rev. d'Intelligence Artif. 33.1 (2019): 45-48.

[11]. Chaitanya, Kosaraju, et al. "Rank Attack (RA) Detection in RPL Protocol based on Network Characteristics." 2023 8th International Conference on Communication and Electronics Systems (ICCES). IEEE, 2023.

[12]. Lakshman Narayana Vejendla and Bharathi C R, (2018), "Effective multi-mode routing mechanism with master-slave technique and reduction of packet droppings using 2- ACK scheme in MANETS", Modelling, Measurement and Control A, Vol.91, Issue.2, pp.73-76.

[13]. Santhi Sri, K., Sandhya Krishna, P., Lakshman Narayana, V., Khadherbhi, R. (2021). Traffic Analysis Using IoT for Improving Secured Communication. In: Reddy, A., Marla, D., Favorskaya, M.N., Satapathy, S.C. (eds) Intelligent Manufacturing and Energy Sustainability. Smart Innovation, Systems and Technologies, vol 213. Springer, Singapore. https://doi.org/10.1007/978-981-33-4443-3_48

[14]. Kumari, G. R. P., Jahnavi, M., Harika, M., Pavani, A., & Lakshmi, C. V. (2023). Smart traffic signal control system using artificial intelligence. In Intelligent Communication Technologies and Virtual Mobile Networks (pp. 829-838). Singapore: Springer Nature Singapore.

[15]. Naresh, A., TSLP, H., Ch, G., & Kumari, G. R. P. (2023, July). Early Prophecy of Low-Birth-Weight Babies Using BM Error Rate Classifier. In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp.1-6). IEEE.

[16]. P. S. Krisha and S. R. Peram, "A Brief Survey on Image Denoising based Feature Extraction and Classification Models for Oral Cancer Detection," 2023 International Conference on Sustainable

Computing and Data Communication Systems (ICSCDS), Erode, India, 2023, pp. 702-708, doi:10.1109/ICSCDS56580.2023.10104790.

[17]. Rao, S. S., Rao, P. N., Babu, R. M., & Ramakrishna, K. V. S. S. (2024). A GAME THEORETIC COGNITIVE SPECTRUM SENSING SCHEME FOR IoT NETWORKS. Telecommunications and Radio Engineering, 83(9).

[18]. Chaitanya, Prathipati Silpa, et al. "Distracted Driver Detection using Inception V1." 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC). IEEE, 2023.

[19]. B. Nobel, Y. Altinkaya, and K. Yildiz, "Federated Learning in Intrusion and Fraud Detection: Current Trends and Future Directions," Cluster Computing, 2025.

[20]. L. Chen, M. Zhao, and H. Wang, "Federated XGBoost with Secure Gradient Aggregation for Credit Card Fraud Detection," IEEE Transactions on Artificial Intelligence, vol. 6, no. 8, pp. 9123–9135, 2025.

[21]. Kavishwar, S. (2011). Pension funds as an infrastructure financing avenue: An exploratory study. *Management Dynamics*, *11*(2), 33-45.

[22]. Bidwaikar, V. N., & Kavishwar, D. S. (2012). Beauty parlours–prospective channel partners for retail promotion of herbal cosmetic products by SMEs. *Indian Streams Research Journal*. 2(1), 1-4

[23]. Shahu, A., Tiwari, H., Joshi, M., & Kavishwar, S. An Analysis of the Effectiveness of Index ETFS and Index Derivatives in Covered Call Strategy. *Journal of Informatics Education and Research*. 4(3), 42-48.

[24]. Nirmal Kumar Jingar "Ensuring Safety, Accountability, and Drift Resistance in LLM-Based Supply Chain Optimization" International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 10, Issue 1, pp.472-482, January-February-2023. Available at doi : https://doi.org/10.32628/IJSRSET2310372

[25]. Jingar, N. K. (2026, February 13). Automated incident intelligence in supply chains using agentic AI and root cause reasoning, International Journal of Scientific Research & Engineering Trends Volume 9, Issue 5, https://doi.org/10.5281/zenodo.18162511

[26]. Nijim, M., Kanumuri, V., Alaqqad, W., Albataineh, H. (2023). Advanced Traffic Management System for Smart Cities. In: Daimi, K., Al Sadoon, A. (eds) Proceedings of the 2023 International Conference on Advances in Computing Research (ACR'23). ACR 2023. Lecture Notes in Networks and Systems, vol 700. Springer, Cham. https://doi.org/10.1007/978-3-031-33743-7_19

[27]. Nijim, M., Kanumuri, V., Al Aqqad, W., Albataineh, H. (2024). Machine Learning Based Analysis of Cyber-Attacks Targeting Smart Grid Infrastructure. In: Daimi, K., Al Sadoon, A. (eds) Proceedings of the Second International Conference on Advances in Computing Research (ACR'24). ACR 2024. Lecture Notes in Networks and Systems, vol 956. Springer, Cham. https://doi.org/10.1007/978-3-031-56950-0_28

[28]. Racha, Ganesh. "Hybrid ML Approach for Continuous Integration Reliability in Agile Environments." United International Journal of Engineering and Sciences (UIJES), vol. 5, no. 3, 2025, pp. 9–21.

[29]. Racha, Ganesh. "Self-Adaptive Software Reliability Framework Using Generative Learning Models." International Journal for Modern Trends in Science and Technology, vol. 12, no. 1, 2026, pp. 30–37.

[30]. Veginati, Navya. "Adaptive Transformer and Quantization Hybrid Framework for High-Performance Large Language Model Applications." United International Journal of Engineering and Sciences, vol. 5, no. 4, Dec. 2025, pp. 46–56

[31]. Veginati, Navya. "Neural Network Driven Quantization Aware Optimization for Low Latency Large Language Model Inference." International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 10, no. 3, May-June 2024, pp. 1162–1170, doi:10.32628/CSEIT25113584.

[32]. Jonnalagadda, P.K. (2026). Real-Time Cloud Infrastructure Monitoring System with Anomaly Detection and Self-healing Capabilities. In: Kumar, V.N., Senkerik, R., Prasad, V.K., Kumar, T.K. (eds) Intelligent Computing and Communication. ICICC 2025. Lecture Notes in Networks and Systems, vol 1839. Springer, Cham. https://doi.org/10.1007/978-3-032-18349-1_43

[33]. Jonnalagadda, Pawan Kalyan. "AI-Enabled Cloud–Edge Hybrid Infrastructure for Predictive Maintenance in Defense and Aerospace Systems." International Journal of Science, Engineering and Technology, vol. 12, no. 2, 2024.

[34]. Ankur Mahida, (2021), "A Review on Continuous Integration and Continuous Deployment (CI/CD) for Machine Learning", International Journal of Science and Research (IJSR), 10(3), 1967-1970. https://dx.doi.org/10.21275/SR24314131827, https://www.ijsr.net/getabstract.php?paperid=SR24314131827

[35]. "Mahida, A. (2022). Comprehensive Review on Optimizing Resource Allocation in Cloud Computing for Cost Efficiency. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-249. DOI: doi. org/10.47363/JAICC/2022 (1), 232, 2-4."

[36]. Tummuri, S. S. R. (2024). Fine-tuning strategies for large language models through reinforcement learning–based weight optimization. International Journal of Science, Engineering and Technology. Volume 4, Issue 3.

[37]. Tummuri, S. S. R. (2024). Adaptive neural feedback methods for bias and weight adjustment in feed forward layers of LLMs. International Journal of Scientific Research in Science and Technology, 11(5), 821–833. https://doi.org/10.32628/IJSRST52310380

[38]. Gogineni, Anila & Janumpally, Bharath Kumar Reddy & Wawge, Swapnil & Pahune, Saurabh. (2025). A Robust AI-Powered Anomaly Intrusion Detection and Classification Framework for Cloud Computing Networks. 1-6. 10.1109/INDISCON66021.2025.11253743.

[39]. A. Joon, B. K. R. Janumpally, A. Gogineni and P. Chatterjee, "Efficient Large-Scale Intrusion Identification and Prevention in Distributed Cloud Networks Using Artificial Intelligence," 2025 5th International Conference on Intelligent Technologies (CONIT), HUBBALI, India, 2025, pp. 1-8, doi: 10.1109/CONIT65521.2025.11167760.

[40]. Arora AS, Yachamaneni T, Kotadiya U. A Comprehensive Analytical Framework for Modeling Consumer Credit Card Behavior and Risk Profiling Using Advanced Financial Metrics. IJAIDSML [Internet]. 2022 Jun. 30 [cited 2026 Apr. 2];3(2):90-100.

[41]. Arora AS, Yachamaneni T, Kotadiya U. Optimizing Multi-Tenant Resource Allocation in Cloud-Based Distributed Systems for Large-Scale AI Model Training Using In-Memory Computing. IJERET [Internet]. 2021 Mar. 30 [cited 2026 Apr. 2];2(1):37-46.